APPARATUS AND METHOD FOR EFFICIENT MODULAR EXPONENTIATION

ABSTRACT OF THE DISCLOSURE

An improved apparatus and method for modular multiplication and exponentiation to achieve efficient computation involved in Montgomery multiplication is provided. Currently employed conventional iteration methods involve carry look-ahead additions. To overcome the time taken by carry look-ahead additions, there is thus provided, in accordance with a preferred embodiment of the present invention, an apparatus and method for separately storing and tracking the sum and the carry of the addition involved in Montgomery multiplication. In such a manner, the present invention achieves fast addition times since they are not dependent on the time to compute the carries. As a result, the iterations are carried out much faster than previously possible. By representing the value *A* in the Montgomery multiplication algorithm with a redundant notation, the sum and the carry of the addition are separately stored and tracked, thereby avoiding the delays involved in the computation of the carries. In such a manner, by separately storing and tracking the sum and the carry of the addition, this carry-save addition enables a much faster computation involved in Montgomery multiplication.